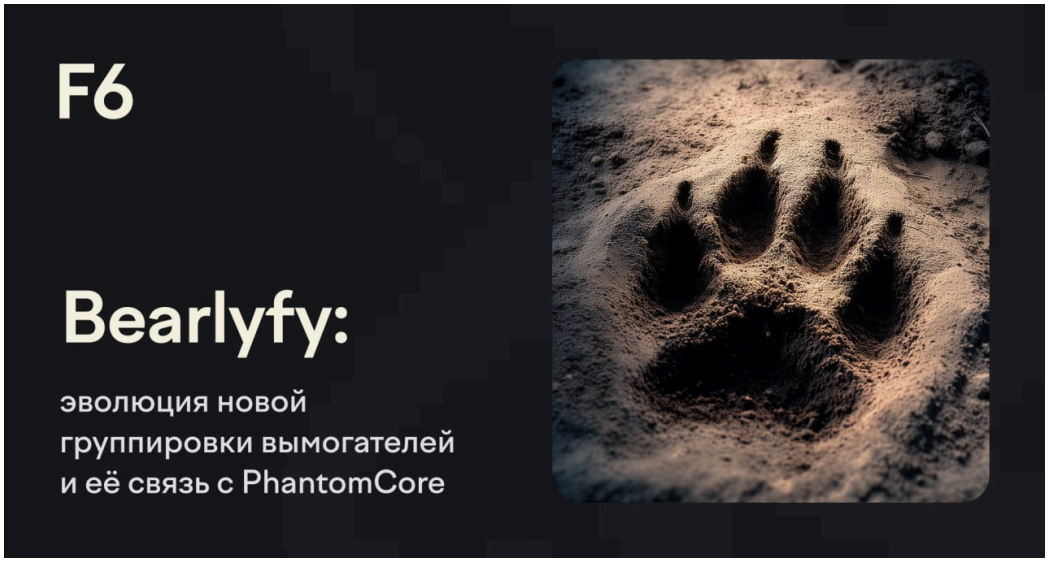
Bearlyfy: эволюция новой группировки вымогателей и её связь с PhantomCore



В последние годы программы-вымогатели продолжают оставаться одной из наиболее значимых киберугроз, эволюционируя как по технической составляющей, так и по модели атак. Одним из новых участников этой сцены стала группировка Bearlyfy, впервые зафиксированная в начале 2025 года. Несмотря на использование уже известных семейств программ-вымогателей, таких как LockBit 3 (Black) и Babuk, группировка демонстрирует собственные подходы к атакам, постепенно увеличивая масштабы своей деятельности.

Исследование, проведённое специалистами F6 Threat Intelligence, позволило проследить динамику развития Bearlyfy: от первых атак на малые компании с относительно скромными требованиями выкупа до сложных кампаний против крупных промышленных предприятий. Анализ тактик, техник и процедур (TTPs) выявил как уникальные черты группировки, так и пересечения с инфраструктурой другого известного игрока — PhantomCore.

Авторы выражают благодарность за помощь при написании блога специалистам Лаборатории цифровой криминалистики и исследования вредоносного кода компании F6.

Первые атаки Bearlyfy

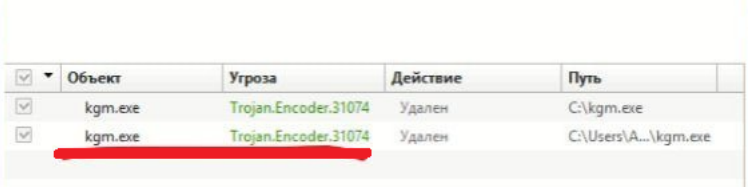
В январе 2025 года специалистами F6 в ходе ежедневного мониторинга на публичной песочнице был обнаружен образец программы-вымогателя (SHA1: 7d5a7965fe464b391daf0d36dfb862d7f53c7728), представляющий собой LockBit 3 (Black),изменяющий расширение файлов после шифрования на “.FHxVySiem”. Файл был загружен из Москвы 15 января 2025 года.

11 февраля 2025 года были обнаружены два новых образца LockBit 3 (Black) (SHA1: bdf776d83aaf85931d2cf2bc53ae5606fcac8f81) и Babuk (SHA1: 2d66caeb7d4fd81ea47b3286fce1ad66a939d0d4). Стоит отметить, что конфигурационные файлы программ-вымогателей, представляющих собой LockBit 3 (Black), идентичны и уникальны.

Анализ ВПО опубликован на платформе MDP F6 (F6 Malware Detonation Platform).

17 февраля 2025 года, был обнаружен новый сэмпл, также имеющий сходства с рассмотренными ранее (SHA1: ade71388dc2fbcb33e69406e88e26d67cd43fa67).

А уже 25 февраля на форуме Kaspersky Club было опубликовано сообщение об атаке вируса-шифровальщика (SHA1: 4268bfee48695e1625d96e9eb904bb14d2eac6dd):



Объект	Угроза	Действие	Путь
kgm.exe	Trojan.Encoder.31074	Удален	C:\kgm.exe
kgm.exe	Trojan.Encoder.31074	Удален	C:\Users\A...\kgm.exe

Рис.1 – Результат сканирования компьютера жертвы бесплатной утилитой

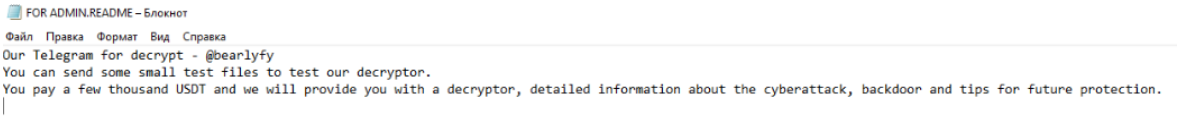
Программа-вымогатель представляла собой LockBit 3 (Black).

Интересной особенностью являлось то, что в настройках конфигурационных -файлов, обнаруженных образцов, не было текста записки о выкупе, из-за чего первоначально предполагалось, что целью атаки является уничтожение данных. Однако позднее было установлено, что злоумышленники создают записку вида «*.README» вручную, в следствие чего в белый список расширений в конфигурационном файле добавлено имя «readme», данная особенность является одним из характерных признаков LockBit 3 (Black), используемых группировкой.

```
"config": {
  "settings": {
    "encrypt_mode": "auto",
    "encrypt_filename": false,
    "impersonation": false,
    "skip_hidden_folders": false,
    "language_check": false,
    "local_disks": true,
    "network_shares": true,
    "kill_processes": true,
    "kill_services": true,
    "running_one": false,
    "print_note": false,
    "set_wallpaper": false,
    "set_icons": true,
    "send_report": false,
    "self_destruct": false,
    "kill_defender": true,
    "wipe_freespace": false,
    "psexec_netspread": false,
    "gpo_netspread": false,
    "gpo_ps_update": false,
    "shutdown_system": false,
    "delete_eventlogs": true,
    "delete_gpo_delay": 0
  },
  "white_folders": "sysvol;0x41471897;$recycle.bin;config.msi;$windows.~bt;$windows.~ws;windows;policies;scripts;boot;program files;program files (x86);programdata;system volume
  "white_files": "autorun.inf;boot.ini;bootfont.bin;bootsect.bak;desktop.ini;iconcache.db;ntldr;ntuser.dat;ntuser.dat.log;ntuser.ini;thumbs.db",
  "white_extens": "386;adv;ani;bat;bin;cab;cmd;com;cpl;cur;deskthemepack;diagcab;diagcfg;diagpkg;dll;drv;exe;hlp;icl;icns;ico;ics;idx;ldf;lnk;mod;mpa;msc;msp;msstyles;msu;nls;nom
  "white_hosts": "",
  "kill_processes": "sql;oracle;ocssd;vmms.exe;vmwp;vmwp.exe;vmcompute.exe;rhs.exe;iscsidcb.exe;dbsnmp;vmms;vmcompute;rhs;iscsidcb;synctime;agntsvc;isqlplussvc;xfssvccon;mydesktop
  "kill_services": "vss;vmcompute;vmms;sql;svc$;memtas;mepocs;msexchange;sophos;veeam;backup;AVP;KAVFS;WinDefend",
  "gate_urls": "",
  "impers_accounts": "",
  "note": ""
}
```

Рис. 2 – Конфигурационный файл обнаруженного образца

Изначально злоумышленники атаковали небольшие российские компании, а средняя сумма выкупа составляла несколько тысяч долларов. В одной из первых записок о выкупе содержалась отсылка к учетной записи в мессенджере Telegram с именем bearlyfy. Это и послужило поводом дать такое название группировке.



FOR ADMIN.README – Блокнот

Файл Правка Формат Вид Справка

```
Our Telegram for decrypt - @bearlyfy
You can send some small test files to test our decryptor.
You pay a few thousand USDT and we will provide you with a decryptor, detailed information about the cyberattack, backdoor and tips for future protection.
```

Рис.3 – Первый обнаруженный образец записки с требованиями выкупа

Расширение масштабов: атаки на крупные компании

Со временем, сохраняя высокий темп атак, группировка продолжала наращивать аппетиты и перешла с маленьких компаний на более крупные.

Так, в апреле 2025 года группировка атаковала российскую нефтяную компанию, где в ходе атаки была использована программа-вымогатель семейства LockBit 3 (Black) для шифрования данных на системах под управлением ОС Windows и программа-вымогатель семейства Babuk для шифрования данных на гипервизорах, отличительными особенностями которого являются:

- В зависимости от параметров командной строки программа-вымогатель может функционировать в качестве демона
- Может перед шифрованием завершать процессы ESXi с помощью esxcli
- Создаёт пустые README_TO_RESTORE.txt
- Записывает статистику в /tmp/lock4.log

Во втором случае запуск осуществлялся в сессии локальной учетной записи при помощи PowerShell- скрипта и вспомогательного файла со списком IP-адресов систем. Доступ к учетной записи осуществлялся по протоколу удаленного рабочего стола (RDP).

В ходе исследования удалось обнаружить, что в конфигурационном файле LockBit 3 (Black) включено самораспространение через Admin Shares (PsExec), а текст записки с требованиями выкупа был изменен и стал содержать ссылку на мессенджер Simplex (рис. 4).

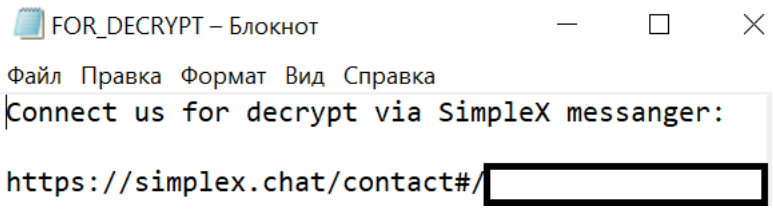


Рис.4 – Видоизмененный образец записки с требованиями выкупа

Уже в июне 2025 года группировка Bearlyfy атаковала российские консалтинговую и инжиниринговую компании. Как и в апрельской атаке, группа использовала программы-вымогатели из семейств Babuk и LockBit 3 (Black) . При этом стоит отметить, что используемый в данной атаке образец Babuk идентичен тому, что использовался группировкой в апрельской атаке. Записка с требованиями выкупа была также изменена.

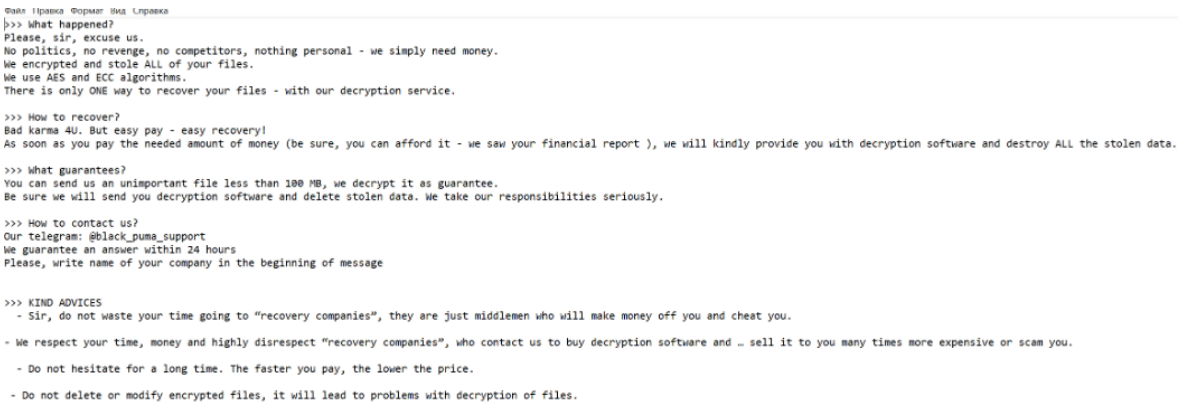


Рис.5 – Третий вариант записки с требованиями выкупа

В июле 2025 года группировка Bearlyfy атаковала российскую строительную компанию. По имеющимся данным, специалистами F6 было установлено, что злоумышленники зашифровали данные компании и запросили выкуп в размере 80000 евро.

В ходе данной атаки доставка и исполнение программы-вымогателя на системах Windows осуществлялись тремя способами:

1. Доставляли с помощью буфера обмена и запускали вручную в контексте RDP-подключений.
2. Создавали задание планировщика, с помощью которого осуществлялась доставка и запуск вымогателя.
3. Запускали с помощью PowerShell, шифруя по SMB нетронутые ранее системы.

Таким образом, на момент августа 2025 количество жертв группировки, выявленное специалистами F6, составляет не менее 30, а аппетиты злоумышленников заметно выросли, в последней зафиксированной атаке злоумышленники запросили 80 тысяч евро в криптовалюте, в то время как в первой атаке размер выкупа составлял несколько тысяч долларов. Из-за сравнительно невысоких сумм выкупа в среднем каждая пятая жертва покупает у злоумышленников декрипторы.

Описание типовых атак группировки

При исследовании вышеуказанных атак, специалистами F6 были проанализированы способы первоначального доступа злоумышленников в систему жертв.

Так, в июньской атаке на консалтинговую компанию, вектором первоначального доступа стала уязвимая версия Bitrix. Для повышения привилегий и перемещения внутри периметра злоумышленники использовали уязвимость Zerologon (контроллер домена под управлением уязвимой версии Windows Server). Стоит отметить, что наряду с RDP злоумышленники активно используют WinRM, а также PsMapExec (инструмент

для перемещения внутри периметра в Windows и Active Directory). Атакующие также использовали следующие утилиты:

- Скрипт PowerShell для инсталляции cloudflared и gost
- Клиент Cloudflare Tunnel, cloudflared
- Прокси-туннель gost
- Утилита WinSW

«Утилита *WinSW* позволяет запускать произвольное приложение в качестве системной службы *Windows*»

При анализе июньской атаки на российскую инжиниринговую компанию специалисты F6 обнаружили ряд событий, наиболее ранние из которых относятся к январю 2025 года. Атакующие осуществляли подключения по протоколу SMB к серверу с IP-адреса, находящегося в сети смежной компании. Подобные подключения осуществлялись до февраля, когда после одного из них на устройстве была создана служба Windows Time Service для автоматизированного запуска программы w64Time.exe, которая является средством для сетевого туннелирования Cloudflared. В это же время штатной программой Windows Defender был выявлен и заблокирован вредоносный объект icssvc.exe.

Далее при помощи инструментов из набора Impacket на сервере была создана служба WinScHost для запуска второй программы для перенаправления сетевого трафика модифицированной версии ShinySocks — winScHost.exe. Для создания служб использовалась учётная запись локального администратора.

«Программа «winScHost.exe» разработана на основе открытого исходного кода прокси-сервера SOCKS ShinySOCKS v1.3.3 (https://github.com/jgaa/shinysocks). В отличие от оригинальной утилиты программа «winScHost.exe» запускается в качестве системной службы Windows «winScHost». Конфигурация ShinySOCKS содержится в коде программы.»

После закрепления злоумышленники подключились с помощью протокола удалённого рабочего стола (RDP) и учётной записи Администратор с IP-адреса, находящегося в сети смежной компании. Чуть позднее к серверу вновь подключались по RDP с учетной записи через ранее настроенный сетевой туннель.

В промежутке с февраля до июня атакующие не проявляли активности на исследуемых устройствах.

В июне злоумышленники приступили к завершающему этапу атаки. Используя ранее установленный сетевой туннель, они подключились по RDP с учётной записью с правами доменного администратора. В рамках сессии была установлена служба ssh, а также загружены программы cloudflared (cloudflared-windows-amd64.msi) и driverSvc.exe с подконтрольного злоумышленникам сервера 195[.]133[.]32[.]213 при помощи утилиты certutil. Для получения дополнительного канала доступа в инфраструктуру были установлены службы Cloudflared agent и DriverInitService для запуска программ сетевого туннелирования gost (srvhost.exe) и Cloudflared (cloudflared.exe).

«Использованные атакующими программы cloudflared (Cloudflared Tunnel клиент) разработаны на основе открытого исходного кода утилиты cloudflared (https://github.com/cloudflare/cloudflared). Сервис Cloudflare Tunnel предназначен для безопасного подключения локальных ресурсов через сеть интернет к инфраструктуре Cloudflare без использования публичных маршрутизируемых IP-адресов.»

«Атакующие используют модифицированную версию прокси-туннеля gost (GO Simple Tunnel) (https://github.com/ginuerzh/gost). Утилита gost – простой защищенный туннель (https://gost.run/en/). Туннель gost может быть использован в качестве прокси, проброса портов или обратного прокси.»

Далее для поиска привилегированных учётных записей атакующие извлекали данные из журнала Microsoft-Windows-TerminalServices-LocalSessionManager/Operational на контроллере домена при помощи PowerShell.

Что касается июльской атаки, то, вероятнее всего, первоначальный доступ был получен через партнерскую компанию, также группировка завладела двумя привилегированными учетными записями. Далее, злоумышленники подключались к одному из хостов и искали системы администраторов ИТ-инфраструктуры, извлекая записи журналов событий ОС со сведениями о подключениях к данной системе. Для обеспечения резервного канала связи в ИТ-инфраструктуру и для взаимодействия с внутренним контуром атакующие использовали характерный PS-скрипт, с помощью которой они настроили SSH-туннели по 443 порту к подконтрольному им хосту 45[.]158[.]169[.]131.

Инфраструктурные пересечения с PhantomCore

В ходе анализа вышеуказанных IP-адресов, а также иных индикаторов компрометации, полученных в ходе исследования, мы выявили пересечения в инфраструктуре группировки Bearlyfy и PhantomCore.

PhantomCore – группа, атакующая российские и белорусские компании с 2022 года, впервые обнаруженная специалистами F6 в 2024 году. Группа, вероятно, действует в интересах Украины, поскольку несколько тестовых образцов самописных вредоносных программ были впервые загружены на публичную песочницу с территории Украины.

В апрельской атаке группа Bearlyfy использовала MeshAgent (программное обеспечение, которое устанавливается на удалённые устройства и позволяет им подключаться к центральному серверу, для обеспечения удалённого доступа и управления). Анализ семпла позволил выявить список серверов. Проанализировав его, был также обнаружен список MeshCentral:

- nextcloud[.]soft-trust[.]com — 91[.]239[.]148[.]211
- nextcloud[.]1cbit[.]dev — 213[.]232[.]204[.]110
- softline-solutions[.]cloud — 46[.]8[.]71[.]104 — pvec[.]ufolab[.]ovh
- nextcloud[.]trust-sec[.]it[.]com — 194[.]116[.]215[.]36
- austolns[.]pw — 194[.]87[.]253[.]233
- Предыдущие IP-адреса некоторых доменов: nextcloud[.]soft-trust[.]com — 45[.]87[.]246[.]73, nextcloud[.]trust-sec[.]it[.]com — 45[.]153[.]231[.]231

Пример разбора:

На домене nextcloud[.]1cbit[.]dev развёрнут MeshCentral, который мимикрирует под NextCloud: атакующие изменили иконку на другую — NextCloud, на стартовой странице указали строку Nextcloud, а заголовок основной страницы содержит Nextcloud — Login.

Также реальный IP-адрес сервера, где развёрнут MeshCentral (nextcloud[.]1cbit[.]dev), скрыт за облачным сервисом CloudFlare.

Однако на сервере с IP-адресом 213[.]232[.]204[.]110 по порту 443 отдаётся SSL/TLS сертификат, в поле Subject.CommonName которого присутствует вхождение nextcloud[.]1cbit[.]dev.

Часть указанной инфраструктуры использовалась группировкой PhantomCore при проведении атаки на российскую промышленную компанию в марте 2025 года.

IP-адрес 185[.]158[.]248[.]107,используемый в июньской атаке на консалтинговую компанию, также – использовался группой PhantomCore в атаке на российское предприятие в июле 2024.

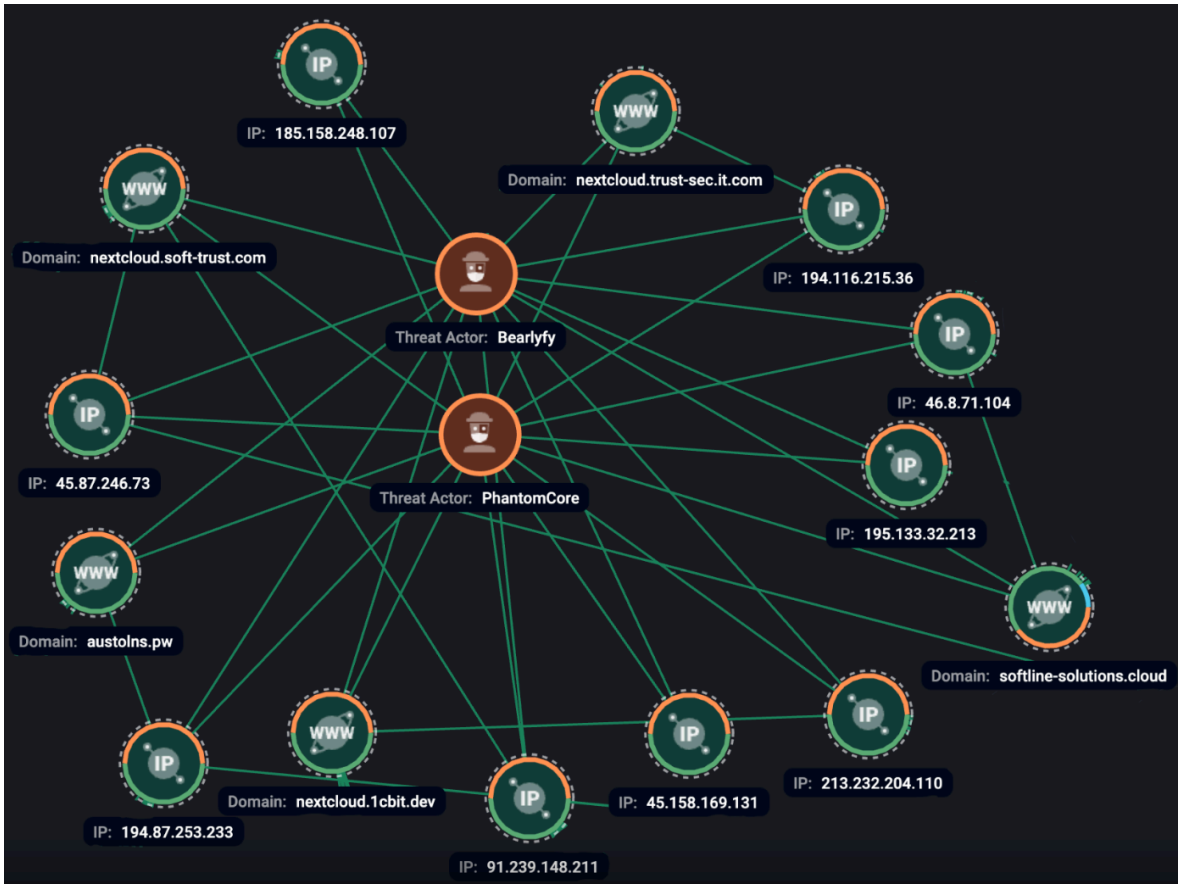


Рис.6 – Пересечения группировок PhantomCore и Bearlyfy, визуализированные с помощью графа F6 TI

Сравнение тактик и техник PhantomCore и Bearlyfy

Несмотря на ряд имеющихся пересечений, проведённый анализ TTPs позволяет выделить два различающихся профиля атакующих. PhantomCore реализует комплексные, многоэтапные атаки, характерные для APT-кампаний. Вектор начального доступа — фишинг и социальная инженерия , с последующим применением специально подготовленных вредоносных компонентов. Группировка широко использует методы уклонения от обнаружения, скрытого присутствия и последовательного развития атаки.

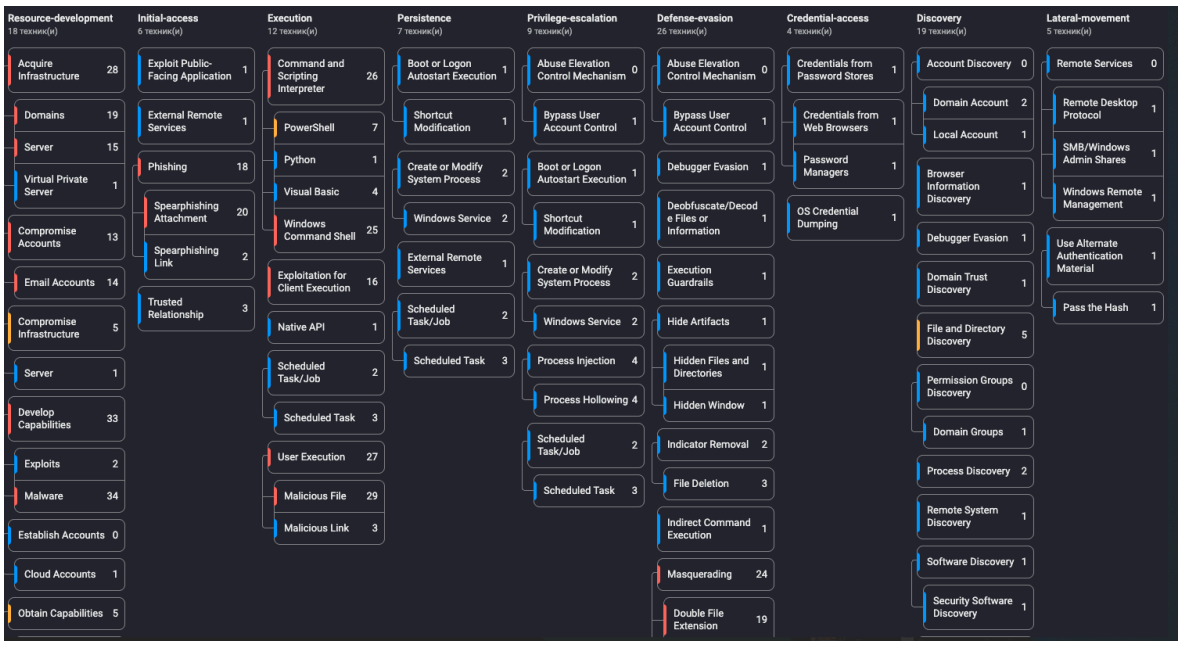


Рис.7-8 – Тактики и техники группировки PhantomCore

Рис.7-8 – Тактики и техники группировки PhantomCore

В свою очередь, Bearlyfy использует иную модель — атаки с минимальной фазой подготовки и прицельным фокусом на достижение немедленного эффекта. Начальный доступ осуществляется через эксплуатацию внешних сервисов и уязвимых приложений. Основной инструментарий направлен на шифрование, уничтожение или модификацию данных. Атаки развиваются быстро, с применением стандартных средств lateral movement и RMM-инструментов (Remote Monitoring and Management). Разведка, закрепление и эксфильтрация не являются приоритетными задачами.

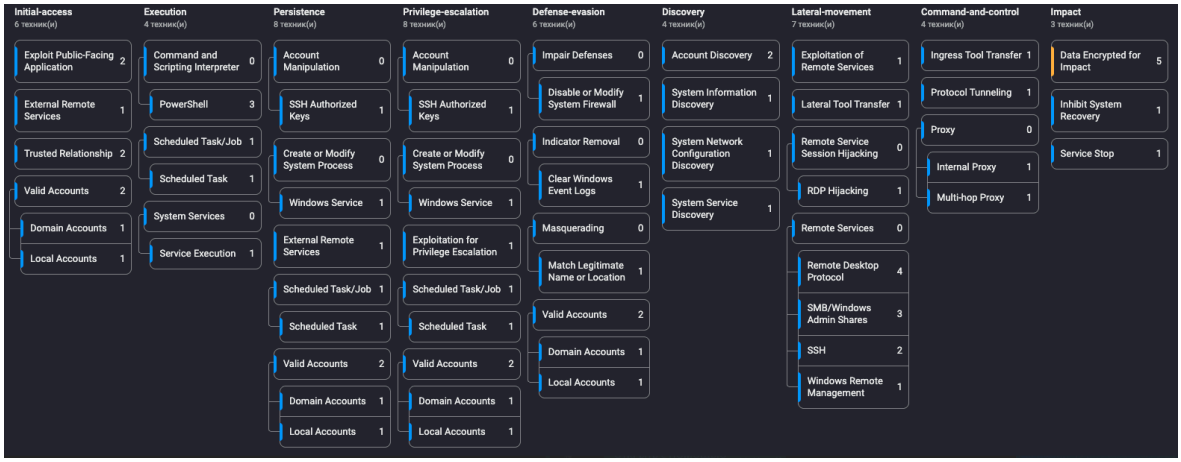


Рис.9 – Тактики и техники группировки Bearlyfy

На основании выявленных различий можно утверждать, что Bearlyfy представляет собой отдельную, автономную структуру.

Вывод

Группировка Bearlyfy, обнаруженная в начале 2025 года, представляет собой новую угрозу в сфере шифровальщиков. Она использует известные программы-вымогатели семейств LockBit 3 (Black) и Babuk. Используемые Bearlyfy инструменты обладают своими характерными особенностями, часть инструментов группировки являются модифицированные версии утилит с открытым исходным кодом. Сама группировка выделяется скоротечными атаками с минимальной подготовкой и оперативным шифрованием данных, также отличительной особенностью атак является то, что записки с требованиями выкупа создаются не программами-вымогателями, а непосредственно атакующими.

Суммы выкупа в зависимости от размера компании варьируются от нескольких тысяч до десятков тысяч евро. По нашим оценкам, каждая пятая жертва выплачивает выкуп. Вследствие низкой проработки атак и ошибочных действий атакующих данные шифруются некорректно. Впоследствии жертвы, которые решили приобрести декрипторы, нередко сталкиваются с проблемами расшифровки.

Bearlyfy использует обычные инструменты для перемещения внутри сети и удалённого управления системами, атакует уязвимые веб-сервисы и Windows, не концентрируясь на скрытом присутствии и эксфильтрации данных. Также были обнаружены отдельные пересечения в инфраструктуре Bearlyfy и PhantomCore, например использование одних и тех же серверов и IP-адресов. При этом подходы к атакам у группировок существенно различаются: PhantomCore проводит сложные, многоэтапные кампании с фокусом на скрытое присутствие и кражу данных, что совсем не похоже на Bearlyfy. Таким образом, Bearlyfy является самостоятельной и независимой группировкой со своей уникальной моделью атак.

Индикаторы компрометации

Файловые индикаторы:

- enc.exe — bdf776d83aaf85931d2cf2bc53ae5606fcac8f81
- ers.exe — 7d5a7965fe464b391daf0d36dfb862d7f53c7728
- e_esxi.out — 2d66caeb7d4fd81ea47b3286fce1ad66a939d0d4
- mig.exe — ade71388dc2fbcb33e69406e88e26d67cd43fa67
- 1v.exe — 4268bfee48695e1625d96e9eb904bb14d2eac6dd
- fwkor.exe — 6c0b7a83ce46e6ffa34ac3fb04cd574bc02ae11d
- qauvy.exe — 5c7a612482a7af27b11f17e2e793c6f3dd856248
- kolhoz.exe — a60d6d6e1745220b143bbfb6b214594cbd1ce8d8
- systemd — 6feaac36d6c9175bd7bbba1279cc6430976e12bd, b8fd7845c0bb56ab786ab9801da4531b81dd12cc
- dnsclient64.exe — 9F8F60E2C3C33EDE923BE622DD60F623A064E6DD
- kernel64-tzar — 835bd6a13ad025a34b85d51ecfd38c1d06f177ea
- SSHService.ps1 — ca7321d8e778310d2b14d6082ac055df7f8c75c2, 4ed37e27932f0db5ff98c8a6f5ea1b3ce078ab7a
- cloudflared.exe — e23d1c937c5e4b1d116010d5c9b1412a59c67b88, 8c7b5a3e82791123b9810b065244ad1f95a3fc6c, 8836d741b13d192b70acdc684ad3fb28b52149ea
- gost.exet — 48fc0f8fe7f8cf20b4db9bd525798e48e5972bce
- dllhost.exe — 59a97f9d7c1d6e10fa41ea9339568fb25ec55e27, e132d57ee2afbb0a1c479631fd70e7df85623642, 0049580250a7b8e65311acb7995450c750afc4c3
- winScHost.exe — 2e75c65977975110c8f7288801eb212f4557d6e0, e838d6ddf4da432de631d0f0120fb94f696150c0, f16f3c7dd300bb403135c0daf38bb163e4707a18
- svchost.exe — ce36d71fbfd9d989a409f8a42a817996d53332d2

Сетевые индикаторы:

- 195[.]133[.]32[.]213
- 45[.]158[.]169[.]131
- nextcloud[.]soft-trust[.]com — 91[.]239[.]148[.]211
- nextcloud[.]1cbit[.]dev — 213[.]232[.]204[.]110
- softline-solutions[.]cloud — 46[.]8[.]71[.]104 — pvec[.]ufolab[.]ovh
- nextcloud[.]trust-sec[.]it[.]com — 194[.]116[.]215[.]36
- austolns[.]pw — 194[.]87[.]253[.]233

- nextcloud[.]soft-trust[.]com — 45[.]87[.]246[.]73
- nextcloud[.]trust-sec[.]it[.]com — 45[.]153[.]231[.]231
- 185[.]158[.]248[.]107